



User Guide to the Smartcard Manager, v1.11

Configuring readers for LEGIC, Felica
and MIFARE cards

RF IDEas, Inc.

January 2021

Table of Contents

1) Scope	2
2) Cards and Keys	2
3) Standard Controls	3
4) General Settings	3
5) LEGIC Settings and Key	4
6) FeliCa Settings	7
7) MIFARE DESFire Settings	10
8) MIFARE DESFire Key	12
9) MIFARE Classic Settings Tab	13
10) MIFARE Plus	15
11) MIFARE Ultralight	17
12) Host Encryption	18
13) MIFARE Key Storage overview	20
rf IDEAS, Inc.	Smartcard Manager v1.11 User Guide

1) Scope

This user guide describes how to use the Smartcard Manager application to configure rf IDEAS readers. Readers that are capable of reading data fields from contactless cards require additional settings beyond our typical interfaces.

For keystroke readers, the Smartcard Manager will inform the reader what data bytes to read and what keys are needed to access that data. Then pcProxConfig can be used for additional formatting of that data, to get the desired keystroke output. For SDK access and MFP24 readers, Smartcard Manager is the only application needed.

Card types currently supported are LEGIC (advant and prime), FeliCa Standard, MIFARE Classic, Plus, Ultralight and DESFire (see table in section 2). Details of the cards are not included here, but a high-level overview is given. It ends with a brief description of how MIFARE keys are stored (in section 12).

NOTE: All numeric entries are in hexadecimal!

2) Cards and Keys

A brief overview of smart cards that can be accessed with Smartcard Manager, 1.7 and appropriate firmware (most firmware will support a subset of this table).

Card Type	Variations Supported	Key type/Protection	Memory layout
LEGIC	Advant (ISO-14443A and ISO-15693), prime	1/2/3/ key 3DES, AES-128, AES-192, AES-256, SAM launch	Segments, accessed by segment number or Stamp ID
MIFARE Classic	Standard, MIFARE Plus at SL1	MIFARE Standard (6-byte) on Key A or B	Blocks (16 bytes) and Sectors (nominally 3 data blocks)
MIFARE Plus	S, SE, C, X at SL3	AES-128	Blocks (16 bytes) and Sectors (nominally 3 data blocks)
MIFARE DESFire	EV1, EV2, LEAF	AES-128, 1K TDEA, 2K TDEA (native)	Applications (AID) containing files of variable size
MIFARE UltraLight	Standard, C, unprotected portion of EV1	None, 2K TDEA	Pages of 4 bytes each
FeliCa	Standard	None, 3DES, AES-128	Blocks of 16 bytes

3) Standard Controls

Some controls can be accessed at all times. The **Configure Reader** button at the bottom will send configuration data (not including keys) to the reader. Next to it is the status bar, where any error condition will be displayed in red.

There are several menu entries, some of which deserve special mention:

1. File | Save Configuration – save configuration settings, including keys, if entered, to the PC
2. File | Load Configuration – retrieve configuration settings from the PC
3. File | Start Trace Log File – captures actual USB messages to and from the reader
4. Options | Perform Beep Test – test the current connection by telling the reader to beep
5. Help | About Smartcard Manager, About Reader – display version and other information

The Save and Load Configuration options creates a readable .ini file for all settings and keys that are currently set in the active tabs. To avoid saving a key in a readable format, it is recommended to use the Encrypt button found in the key tab before saving the configuration.

4) General Settings

In the General Settings tab, **Connect/Reconnect** will establish connections to the reader, useful when switching readers on the PC (it will only connect to one reader at a time). It reads the current configuration of the reader as part of the connection process.

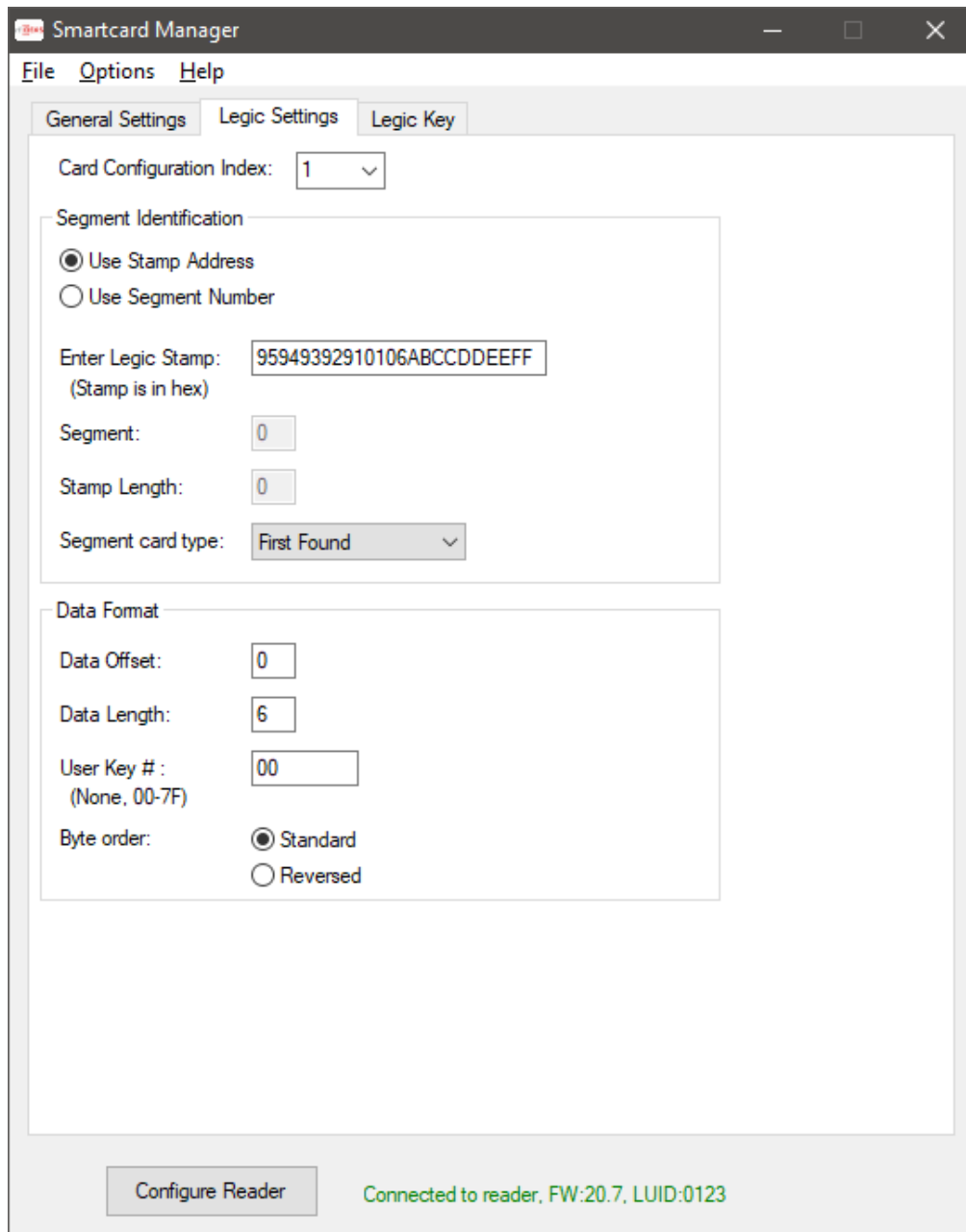
The General Settings tab is used to configure card types, and additional tabs are used to select the specific read/authentication configuration and to send keys. This will establish which bytes to read from the card, and how to access them. The pcProxConfig utility can be used if additional settings are needed for specialized keystroke output, such as converting the data to decimal or ASCII output. There can be multiple secure file configurations set at one time, and a mix of MIFARE card types and/or repeats of a MIFARE card type. LEGIC readers do not read MIFARE secure data and vice versa.

If the same secure file data card type is selected for more than one configuration, then a pull-down Card Configuration Index (1-4) in the subsequent tabs will determine which configuration is currently selected.

For newer readers (after firmware version 22.2), then there is an option to create another tab to set the Host Encryption Key. This key is used to encrypt keystroke card data sent to the host from the reader.

5) LEGIC Settings and Key

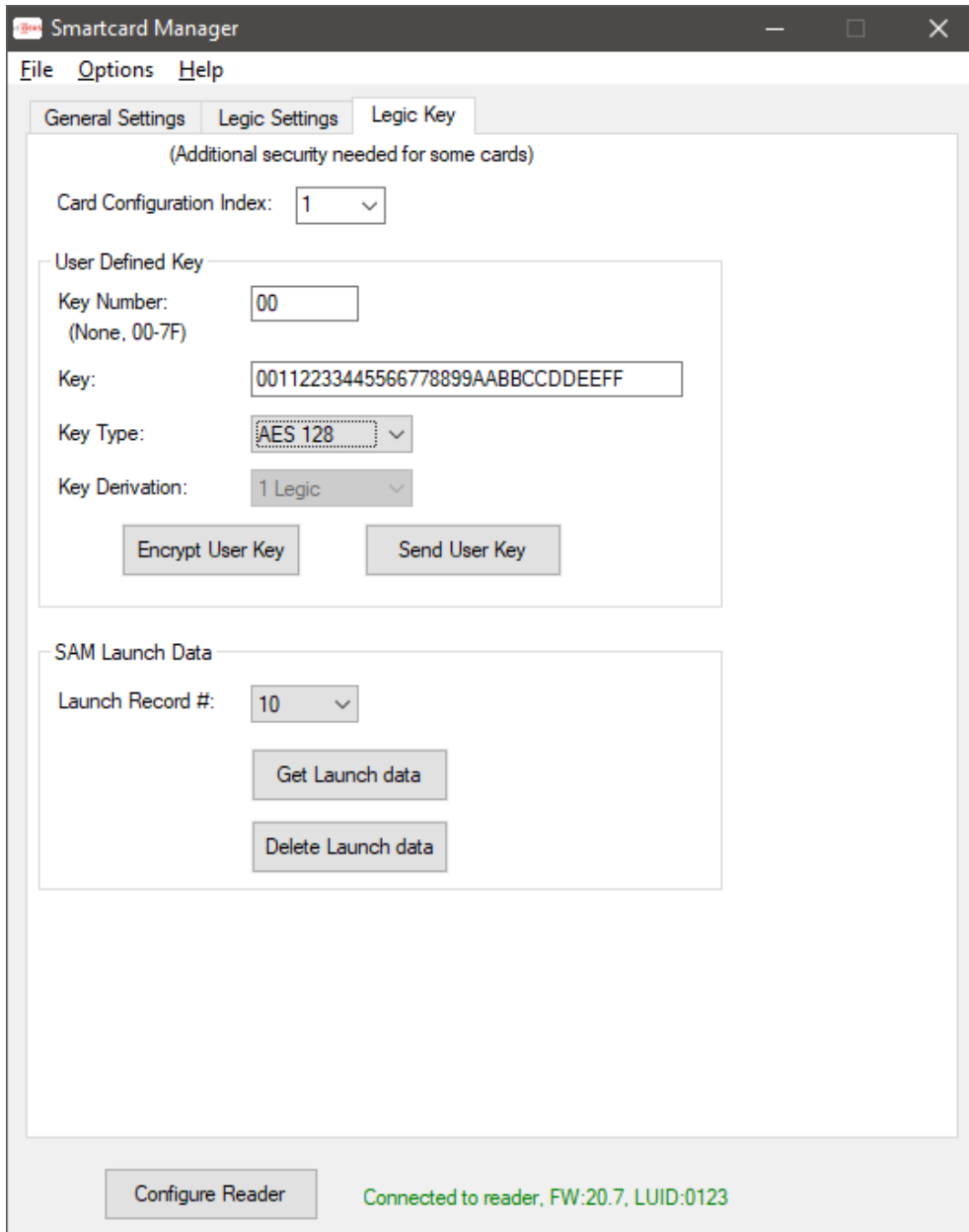
If a card type is set to LEGIC Stamp, then a tab for LEGIC Settings will appear. For firmware version 20.7 and later, a tab for LEGIC Key will also appear. The LEGIC settings tab has the following fields:



A LEGIC segment can be addressed by the Stamp Address, or by the segment number. When using the segment number, an optional Stamp Length field is available. Entering this will keep the data consistent if both LEGIC advant and prime cards are being used, as the prime card includes the stamp with the card data, while the advant does not.

The Segment Card Type field is useful when using a multi-technology LEGIC card. There are three LEGIC technologies: prime, advant on ISO-14443A, and advant on ISO-15693. On a multi-technology card, there will be a combination of technologies, each with its own range of segments, possibly using the same Stamp address. This field will determine which one is used, or "First Found" is non-discriminatory (default case, and best choice for the standard single-technology card).

For firmware versions 20.7 and later, a user-defined key number can be entered. This key number is an index to a table stored in the LEGIC chip. The actual key is entered in the next tab, the LEGIC Key tab.



The key is entered on this tab, and stored at location Key Number in the LEGIC chip. The key cannot be read back. If desired, the key can be encrypted after it is entered. Thereafter it will be displayed in

the encrypted form, stored in the configuration file as encrypted (if a configuration file is created), and it is sent encrypted over USB to the reader.

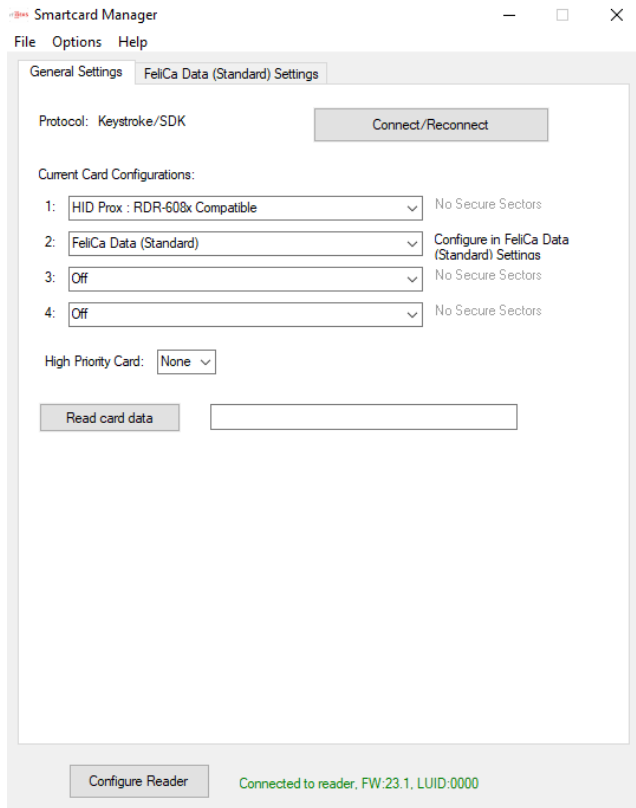
The bottom section of this tab is used for Launch (baptism) using a SAM-63 card. Some user cards require that a reader be launched before the user data can be read. If LEGIC Stamp is selected as a card type, than any LEGIC reader (including 20.5) can be launched with a SAM-63 card.

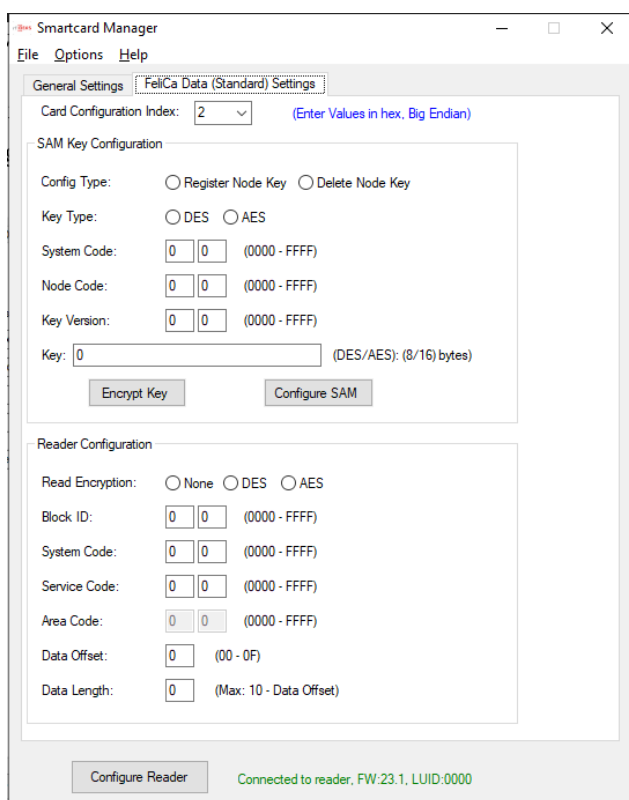
In firmware 20.7 and later, when a SAM-63 card is detected in the field, the usual 15-second window for launching is reduced to 7 seconds, and a beep and/or LED change indicates the launch has occurred. This results in a record being stored in the LEGIC chip. This launch record can be read back, to verify it was launched, and it can also be deleted.

6) FeliCa Settings

If a card type is set to FeliCa Data (Standard), then a tab for FeliCa Settings will appear. This card type is supported for firmware version 23.1. The FeliCa Data (Standard) settings tab has the following fields:

1. SAM Key Configuration
2. Reader Configuration





1. SAM Key Configuration :

Use this section to program Felica Standard Node key into Sony Felica RW-SAM (RC-S500/S02). This is independent of any Card Configuration Index. All fields of this section are disabled if SONY FeliCa RW-SAM is not present in the reader.

Config Type:

Select if you want to register a key or delete a key.

Key Type:

Select the type of the intended key, between DES key or AES key. DES key is of 8 bytes. AES key is 16 bytes.

System Code:

Node Code:

Key Version:

Enter two-byte value of System Code, Node Code and Key Version of the intended Key (Big Endian).

Key:

Enter the actual value of the intended Key (Big Endian).

This field is disabled if Config Type selected is Delete Node Key

*Example : System Code - 0x0018, Node Code - 0x4090, Key Version - 0x0102

SAM Key Configuration

Config Type: Register Node Key Delete Node Key

Key Type: DES AES

System Code: (0000 - FFFF)

Node Code: (0000 - FFFF)

Key Version: (0000 - FFFF)

Key: (DES/AES): (8/16) bytes

SAM Key Configuration

Config Type: Register Node Key Delete Node Key

Key Type: DES AES

System Code: (0000 - FFFF)

Node Code: (0000 - FFFF)

Key Version: (0000 - FFFF)

Key: (DES/AES): (8/16) bytes

Encrypt Key:

After entering the Key, user can encrypt the key using this button.

Once, the key is Encrypted the field will be disabled. To re-enable field, change Key and press tab.

This field is disabled if Config Type selected is Delete Node Key

SAM Key Configuration

Config Type: Register Node Key Delete Node Key

Key Type: DES AES

System Code: (0000 - FFFF)

Node Code: (0000 - FFFF)

Key Version: (0000 - FFFF)

Key: (DES/AES): (8/16) bytes

Configure SAM:

Once all the fields are updated and user is ready to send configuration, press Configure SAM button. During configuration, reader flashes Amber and beeps once..., then on Success: Flashes Green Momentarily and Beeps twice long. Failure: Flashes Red Momentarily and Beeps twice short.

2. Reader Configuration :

Use this section to program the Reader, to read a Block Data of a FeliCa Standard Card. It is based on Card Configuration Index selected. It supports configuration for reading all 3 three types of FeliCa Standard Cards : AES only, DES only, AES/DES

Read Encryption:

Select the Read Method of the intended Block data. Encrypted(AES/DES) or None.

Block ID:

Specify the 2-byte Block ID of the intended Block data to be read (Big Endian). For Example : Block ID – 1 is 0001, Block ID – 256 is 0100

System Code:

Service Code:

Specify the 2-byte System Code and Service Code of the intended Block data to be read (Big Endian).

Area Code:

Specify the 2-byte Area Code of the intended Block data to be read (Big Endian). This field is only used/required, if Read Encryption : DES is selected. For Read Encryption : None and AES, this field is disabled.

Data Offset:

The Block Data is of 16 bytes, starting from byte 0 ... byte 15.

Provide appropriate offset value as per user requirement.

Data Length:

Provide the length of data to be returned by the reader.

Max data length to be read is 16 bytes (0x10), provided Min Data Offset is 0.

Configure Reader:

Once all the fields are updated. Press Configure Reader button, to program the Reader Configuration setting for the chosen Card Configuration Index.

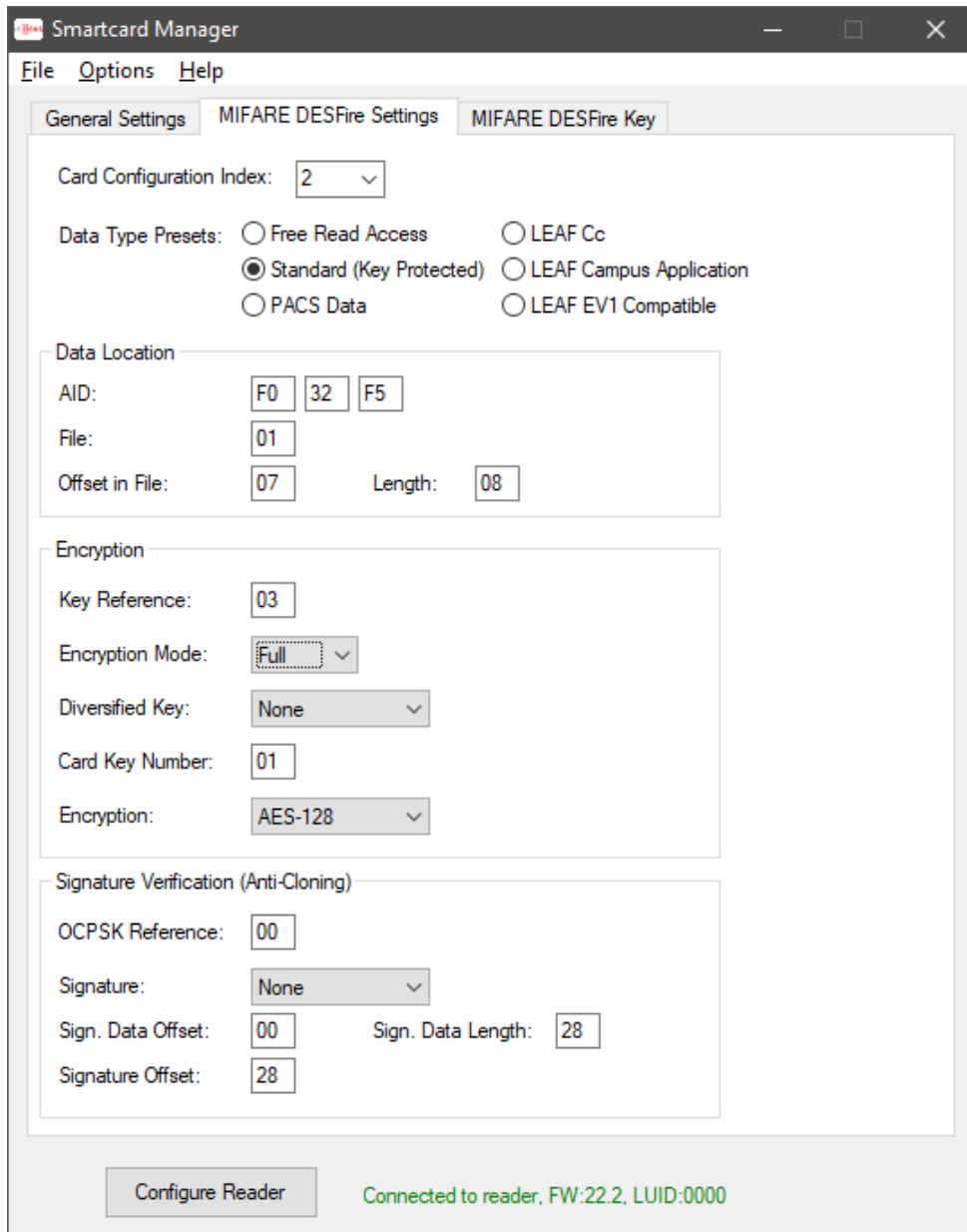
*Example : System Code - 0x0018, Service Code - 0x4090/0x4097, Area Code - 0x4081

The image displays three screenshots of the 'Reader Configuration' interface. Each screenshot shows a form with the following fields: Read Encryption (radio buttons for None, DES, AES), Block ID (two input boxes, range 0000 - FFFF), System Code (two input boxes, range 0000 - FFFF), Service Code (two input boxes, range 0000 - FFFF), Area Code (two input boxes, range 0000 - FFFF), Data Offset (one input box, range 00 - 0F), and Data Length (one input box, range 0 - 10, with a note '(Max: 10 - Data Offset)'). Below the form is a 'Configure Reader' button and a status indicator 'Connected to reader, FW:23.1, LUID:0000'.

- Top Left Screenshot:** Read Encryption is set to **DES**. Block ID: 00 00, System Code: 00 18, Service Code: 40 90, Area Code: 40 81, Data Offset: 00, Data Length: 10.
- Top Right Screenshot:** Read Encryption is set to **None**. Block ID: 00 00, System Code: 00 18, Service Code: 40 97, Area Code: 0 0, Data Offset: 00, Data Length: 10.
- Bottom Screenshot:** Read Encryption is set to **AES**. Block ID: 00 00, System Code: 00 18, Service Code: 40 90, Area Code: 0 0, Data Offset: 00, Data Length: 10.

7) MIFARE DESFire Settings

If a card type is set to MIFARE DESFire Secure File Data, then a tab for MIFARE DESFire Settings will appear. This tab contains the following fields needed for reading a DESFire card:



The Data Type Presets at the top are a handy way to set the reader for common uses. For example, the LEAF Cc and LEAF EV1 Compatible presets will fill in the fields to read the Badge ID from a standard LEAF card. The other options are for more customizable data selection.

The rest of the page is organized into three blocks:

- Data Location – where the data is located on the card, and what bytes to return.
- Encryption – how the data is protected and with what key.
- Signature Verification – for optional anti-cloning protection.

Data Location:

The MIFARE DESFire cards store data in Application spaces, referred to by their Application ID
 rf IDEAS, Inc. Smartcard Manager v1.11 User Guide

(AID). Each AID has one or more Files where the data is stored. The AID is sometimes described in big endian format (most significant number first) or little endian format (least significant number first). Smartcard Manager uses the latter, following the lead of NXP tools, but card documentation may vary.

Encryption

The Key Reference is an index into keys stored on the SAM AV2 chip inserted into the reader. The Key can also be programmed at this time using the DESFire Key tab, or can be programmed at another time, even on a different reader or device. In any case, the Key Reference value on this page must match the Key ID used when storing the key. The index is a value in the range of hexadecimal values 01 to 7F.

A diversified key is modified, in part by the card's CSN, so the resulting key is unique to each card. There are different methods of diversification, some are proprietary to a particular vendor. At this time, the options are:

- None
- Encryption (Classic) which is standard AV1 method
- Encryption UID CKN (AV1, but card key number is part of diversification)
- CMAC UID (AV2 method using only UID for diversification input)

Card key number refers to which key on the MIFARE card is used for access to the data on this AID/File. Typically this is 01, values can be 00 to 0D. Card key number of 0E is reserved for Free Read Access (no key needed).

Key Types:

- AES-128 (uses a 16 byte, 32 character key)
- 2KTDEA-DES (16 byte 3DES using MIFARE DESFire implementation). For single DES, repeat the 8-byte key.
- *2KTDEA-ISO and 3KTDEA (3DES using ISO-10116) are not yet available, as of firmware version 22.2*

Signature Verification

This involves computing a signature from the data and comparing to a value on the card, using a key/process distinct from data encryption. This key used to make the signature is not stored on the card being read, and uses diversification, so a cloned card will fail the signature verification test. The Signature Verification process uses an additional key reference to the Originality and Cloning Protection System Key (OCPSK).

TIMING NOTE: Signature Verification requires additional data to be read and an additional encryption step. On a standard LEAF Cc card for instance, it nearly doubles the read and response time to about 1.5 seconds.

8) MIFARE DESFire Key

Unless the file data is Free Access, a key will be needed to access the data. The key is stored on the NXP AV2 SAM (the removable SIM card). This key is kept separate from reader configuration and other settings. It is not changed if the reader is set to defaults or boot loaded with new firmware. The keys can be programmed onto an AV2 SAM card on one reader, and then the AV2 SAM card can be moved to another reader for use there. (AV2 SAM cards are only recognized at power-on, so the readers will need to be unplugged when moving the cards).

For DESFire, there are two places a key can be used, so there are two sections on this tab. First is Data Access. The AV2 SAM needs the AID stored with the key, so that information is duplicated from the DESFire Settings tab. The second section is for OCSPK, which can use the same key value as above if desired. AID is not needed for the OCSPK.

The screenshot shows the 'MIFARE DESFire Key' configuration window in the Smartcard Manager application. The window has a menu bar with 'File', 'Options', and 'Help'. Below the menu bar are three tabs: 'General Settings', 'MIFARE DESFire Settings', and 'MIFARE DESFire Key'. The 'MIFARE DESFire Key' tab is active. The window contains the following fields and controls:

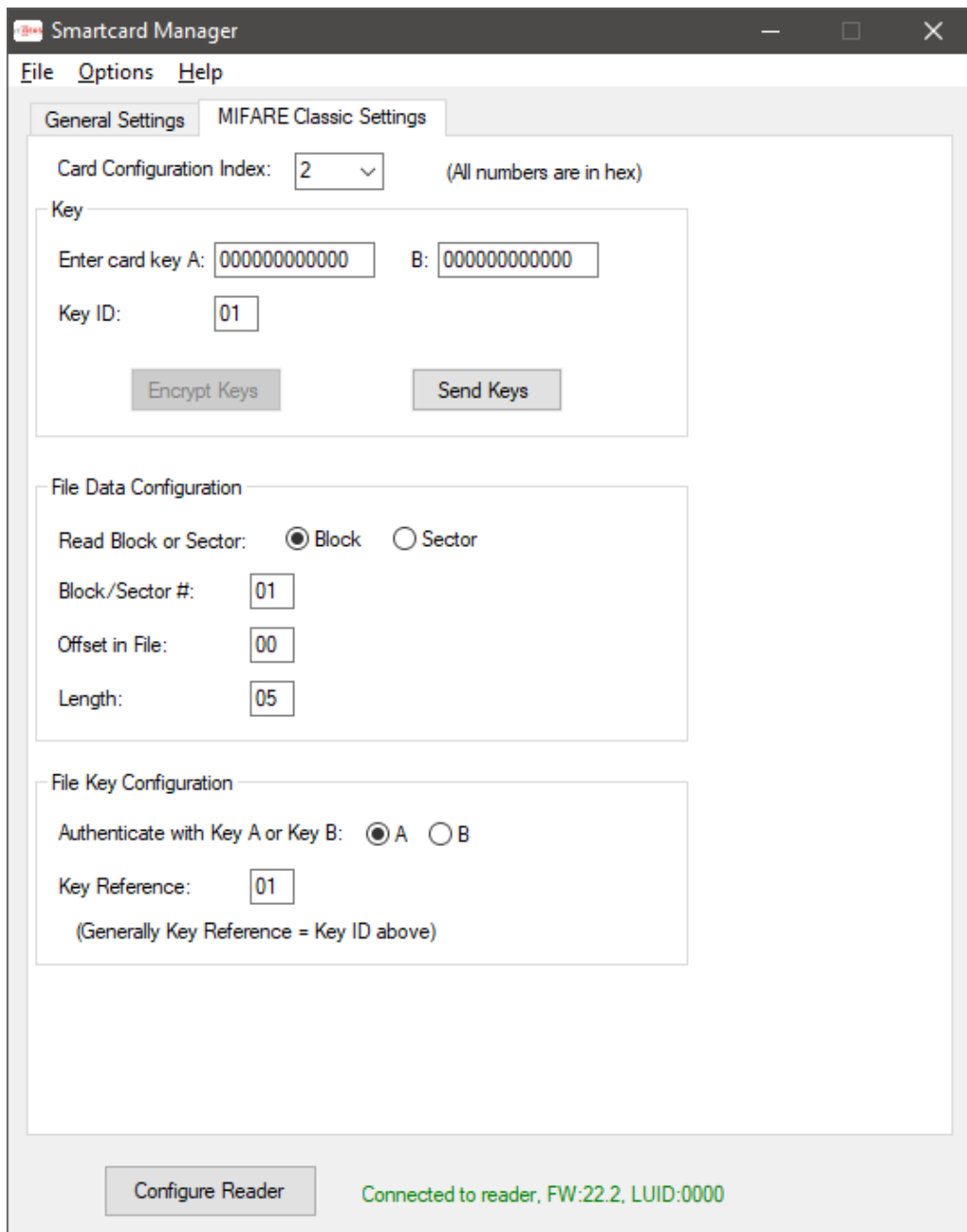
- Card Configuration Index:** A dropdown menu set to '2'.
- Data Access Key to put on SAM in Reader:**
 - Key ID:** A text box containing '03'.
 - Data Access Key:** A text box containing '00112233445566778899AABBCCDDEEFF'.
 - Key Type:** A dropdown menu set to 'AES-128'.
 - AID:** Three text boxes containing 'F0', '32', and 'F5'.
 - Send Key:** A button.
- OCPSK (Anti-cloning key):**
 - OCPSK Key same as Data Access Key
 - OCSPK ID (00=Off):** A text box containing '00'.
 - OCPSK Key:** An empty text box.
 - Key Type:** A dropdown menu set to 'AES 128'.
 - Send OCPSK:** A button.
- Encrypt Keys:** A button.

At the bottom of the window, there is a 'Configure Reader' button and a status indicator that reads 'Connected to reader, FW:22.2, LUID:0000'.

9) MIFARE Classic Settings Tab

The MIFARE Classic card is simpler than the DESFire. Memory is also arranged differently, with sectors composed of blocks. Typically a sector has four blocks: three data blocks, and the last block has key and access information. They count from 0, so block 4 is the first data block of sector 1. Each block has 16 bytes, and each sector has 48 bytes of data.

There are two keys, each 6 bytes long. Typically Key A is used, but Key B is also possible. The two keys fit into one entry in the SAM AV2. Key ID and Key Reference values are the same as in MIFARE DESFire. Note that the Configure Reader button at the bottom of the tab will not send the keys to the reader, there is a separate Send Keys button for that.



Note: The reader firmware has been extended to be able to keystroke up to 48 bytes of data (a typical sector of MIFARE Classic). The SDK (API) interface, however, still has a maximum of 32 bytes. This is only noticeable if the configured length is more than 32 (hexadecimal 20), and the pcProxConfig utility (or similar application using our DLL) is used to retrieve data. The first 32 bytes are returned, and it reports a maximum of 255 bits of data.

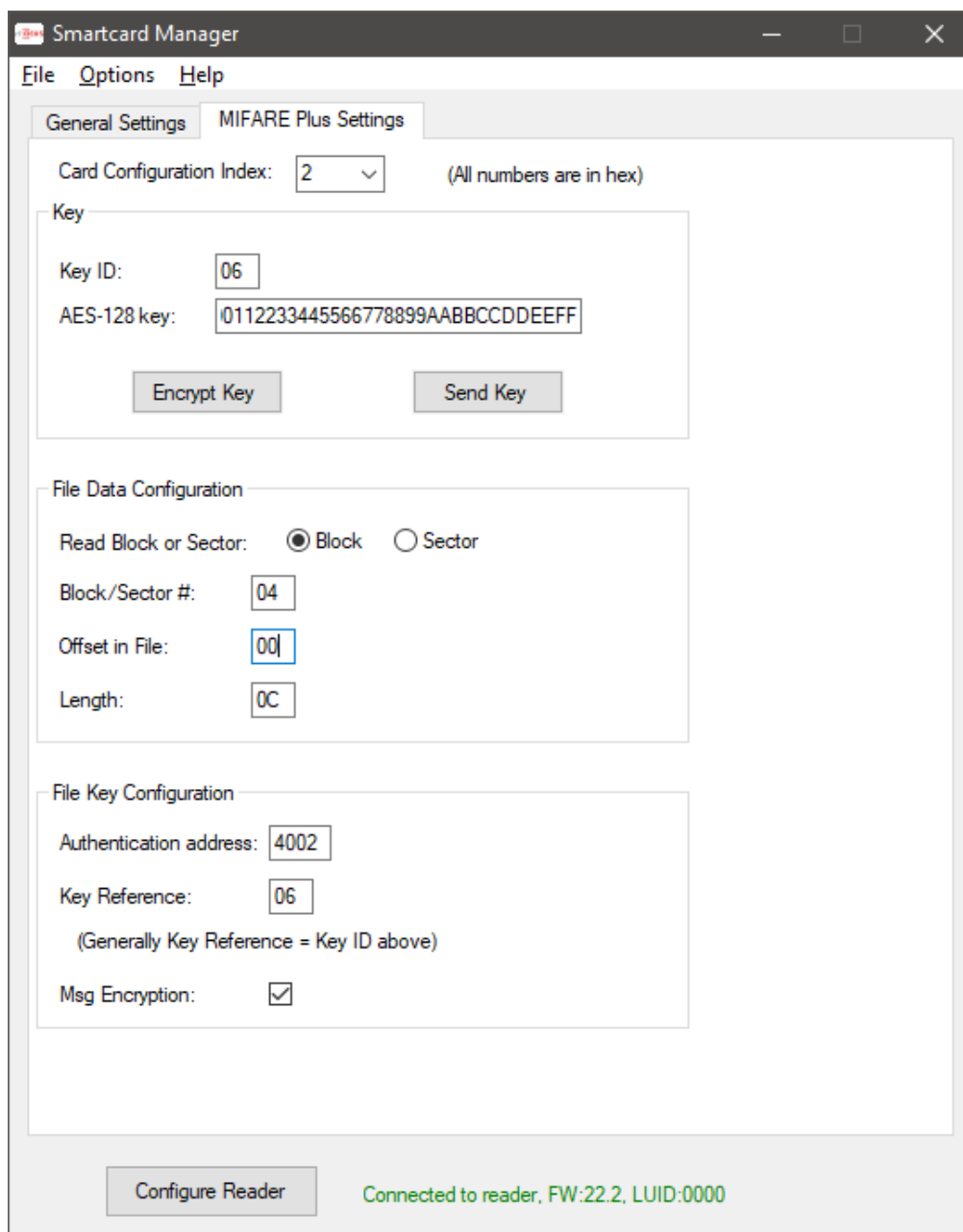
10) MIFARE Plus

MIFARE Plus uses the same memory layout as Classic, with blocks and sectors. Plus has four security levels. Security Level 0 (SL0) is straight from the factory, with no keys programmed. SL1 is in Classic mode and can be read using the MIFARE Classic Secure File card type. SL2 (SL1/SL3 mix mode) isn't currently supported. Choosing MIFARE Plus Secure File card type will allow a card in SL3 mode to be read.

Instead of MIFARE Classic keys (6 bytes), SL3 uses AES-128 keys (16 bytes). It still uses Key A and Key B as authentication options for each sector, but because of memory issues, the keys are moved from the trailing configuration block to a separate Authentication address space.

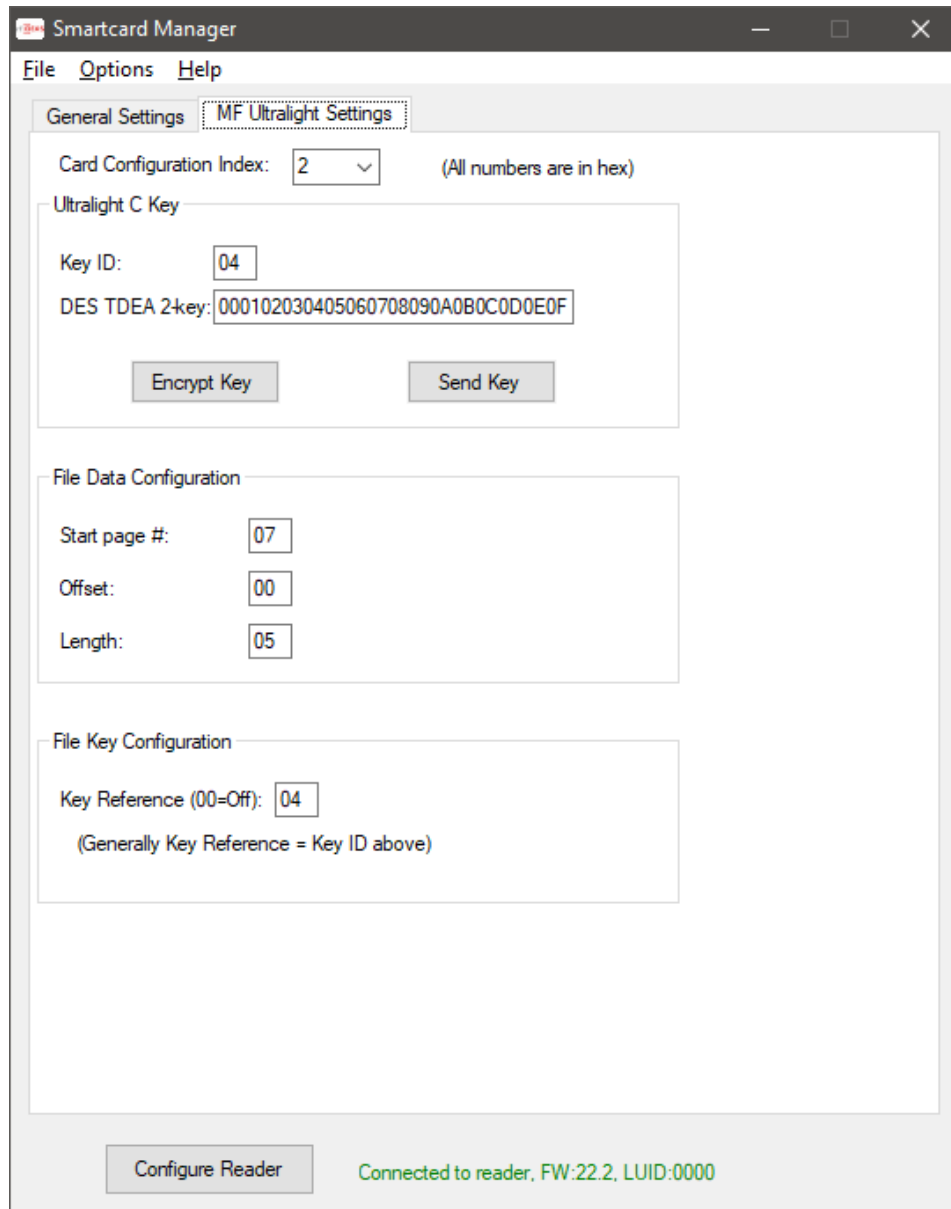
Authentication Address	Sector	Key A/B	Data Blocks (in hex)
0x4000	0	Key A	0-2
0x4001	0	Key B	0-2
0x4002	1	Key A	4-6
0x4003	1	Key B	4-6
0x4004	2	Key A	8-10 (0x08 - 0x0A)
:	:	:	:

Like other secure file configurations, the Key Reference number needs to match the Key ID. These are kept as separate fields because the Key (and associated Key ID) can be written to the NXP SAM AV2 chip at any time, including by a 3rd party at a different location.



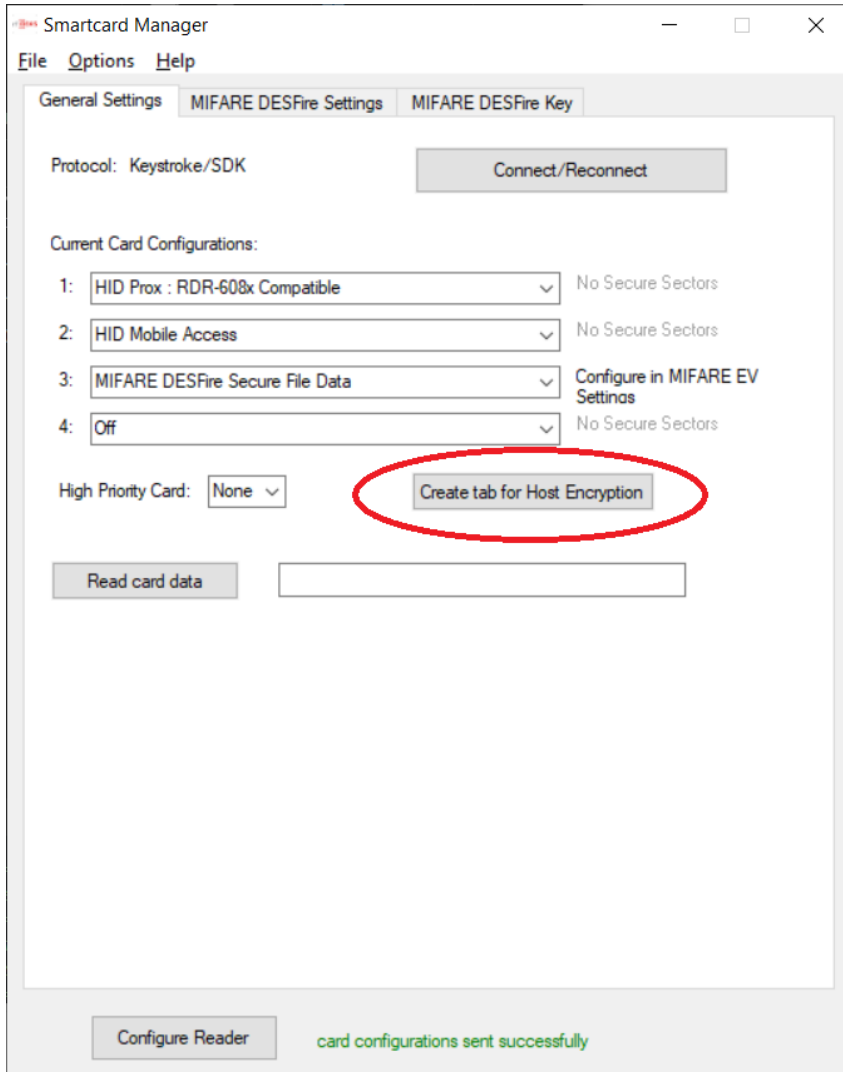
11) MIFARE Ultralight

Ultralight uses Pages of 4 bytes each as the basic memory unit. All flavors of Ultralight can be read if the access rights allow open reads. Ultralight C can be set up to require a TDEA key, so the tab for MIFARE Ultralight Settings includes key information. In many cases a key will not be needed and only the page number, offset and length is needed.

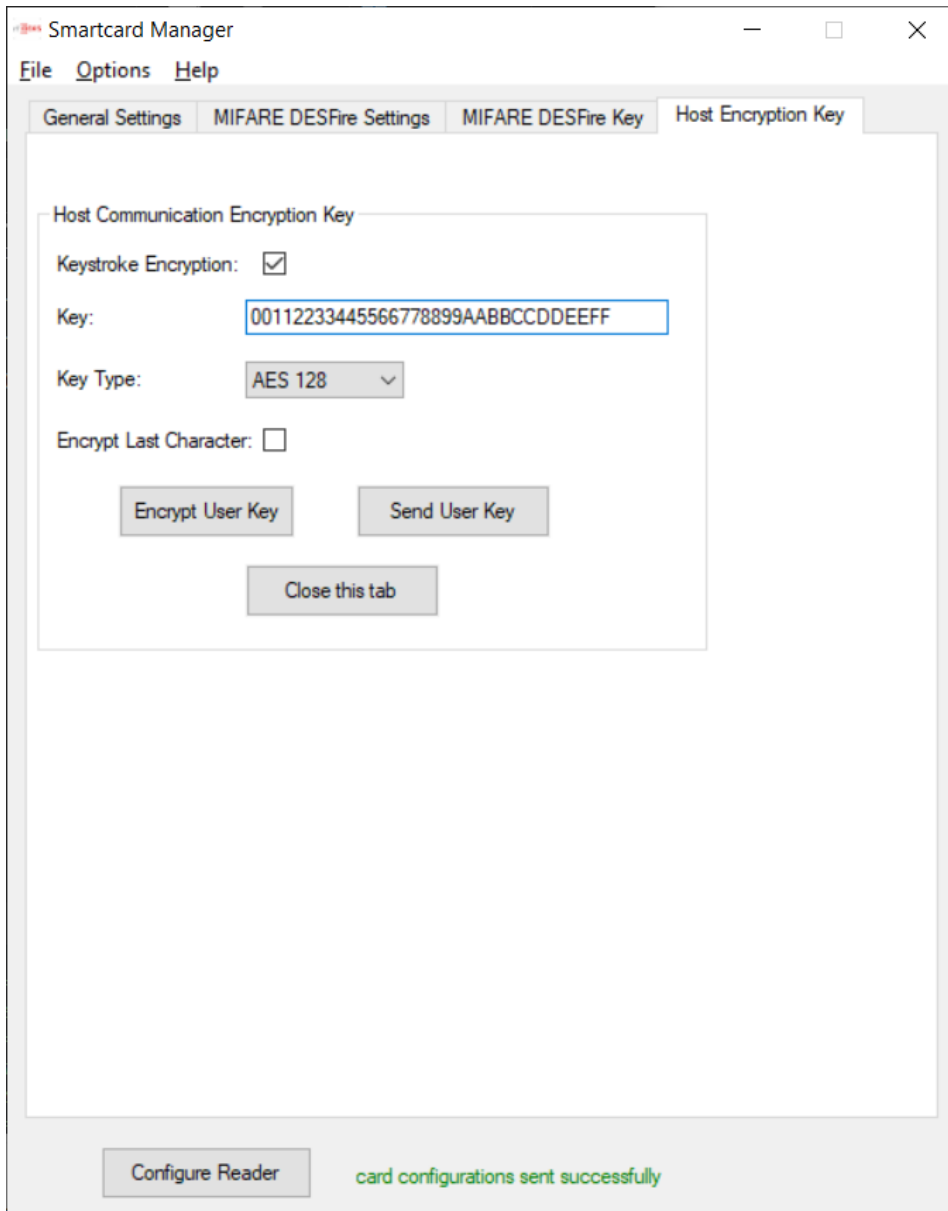


12) Host Encryption

A feature added in reader firmware version 22.3 is encryption of the keystroke output. This applies to all card data being keystroked by the reader, regardless of the type of card that was presented to the reader. There has been a button added to the General Settings tab to create a new tab for these settings.



Clicking that button will open a new tab with the following options:



Keystroke encryption button will enable/disable encryption of keystrokes. The key is currently a 16-byte (32 hexadecimal characters) field, for AES-128 encryption (initial div input of 0x00). Other key types may be available in the future.

Encrypt Last Character is an option for including the final keystroke character - typically a carriage return key - with the encrypted message, or sending that character in the clear. Some host programs need that character in the clear in order to detect the end of transmission.

The data can be decrypted using the same key on the host side, either with our sample `MvxAesDecrypter.Wpf.exe` program, or any number of online AES-128 decryption tools.

The key itself can be encrypted before storing in a local config file or sending to the reader.

13) MIFARE Key Storage overview

The Key ID used when storing a key to the NXP SAM AV2 chip must be the same value that later will be used as the Key Reference when reading the card data. The Key ID has a valid range of 1 to 127 (01 to 7F). MIFARE reserves key 0 as a Master Key. The Card Key Number is an index to the key stored on the card.

See the following figure for specifics on keys. This example uses the MIFARE DESFire card as an example as it is the most complicated. Card key numbers on a DESFire card have a value 0 to 15, with up to 13 keys for each AID. Card key number 14 (0E) is reserved for Free Access, and card key number 15 (0F) is No Access.

